US-PAT-NO: 5534855

DOCUMENT-IDENTIFIER: US 5534855 A

TITLE: Method and system for certificate based alias detection

---------- KWIC ---------

Brief Summary Text - BSTX (4):

User irresponsibility usually refers to situations where an authorized user purposely or accidently causes some noticeable damage. An example would be a computer user who is authorized to access certain computer files, makes an authorized copy of a **key** file to improperly transfer. This type of breach can be characterized as a breach of trust. There is little that a computer operating system can do to protect sites from this source of security failure, since the initial access to the file was completely authorized, and the breach occurred by the improper transfer of the fruits of the authorized access.

Brief Summary Text - BSTX (14):

Moreover, preventing account aliasing becomes more and more impracticable as networks grow larger and larger. Even if identifying information unique to an individual, such as biometric information, is obtained when a **new account is created, in order to associate that new** user account with any other user **account that may exist** for that individual on the network, an exhaustive search over every user account already in the system would have to be performed. Such a search is costly even for relatively small computer networks, and is effectively impossible for large computer networks.

Brief Summary Text - BSTX (20):

In accordance with a further aspect of the present invention, a system of operating a distributed computer system to implement alias detection is provided, including storing in respective user accounts, digitally-signed account certificates including identification information uniquely characterizing each of a plurality of computer users, initiating execution of one stage of a selected transaction program having a plurality of stages from a store of application programs on the computer system upon request from a first user account, processing a request from a second user account to authorize execution of a subsequent stage of the selected transaction program by

comparing the identification information included in account certificates stored in the first user account and in the second user account, determining whether the second user account is an alias of the first user account, and allowing the processing request to execute the subsequent stage of the selected transaction program if the second user account is not an alias of the first user account. With such an arrangement a computer security system which uses a
combination of biometric and **cryptographic** techniques is provided. Specifically it provides a system for supporting a separation of duties policy that is not dependent on a single authority for registering accounts, or rigorous account administration to segregate accounts into different non-overlapping groups or roles (i.e., static enforcement of separation of duties), or preventing multiple accounts for an individual. Such a system embodying the invention can support dynamic enforcement of separation of duties by allowing an individual to assume multiple roles if need be, and ensure that within the context of a given business function, the individual has not assumed conflicting roles. It achieves this by the use of digitized biometric data or other uniquely identifying data to determine if different accounts are used by a single individual, i.e., are aliases of each other.

Detailed Description Text - DETX (6):

Referring now to FIG. 2, an applicant 100 supplies biometric information 105 to a registrar 110 as part of the processing of an account. All accounts in the computer system 10 are administered by the account registrar 110, an entity having its own identity, with responsibility for account administration for some enterprise. During the production or modification of an account, the registrar 110 captures an applicant's biometric information 105. The system uses a public **key encryption** technology for authentication to provide authentication data. The authentication data will be associated with the account for use in login authentication and will be the public **key** of a public **key**/private **key** pair.

Detailed Description Text - DETX (7):

The registrar 110 causes a new public/private **key** pair to be generated. The private **key** is issued to the user (typically in the form of stored information in some device 115 such as a passcard) while the public **key** for the account is stored along with other account information in a so-called "certificate" for that account. The biometric data 105 supplied by the applicant 100 is preferably integrity locked into the certificate along with the authentication data (e.g. user's public **key**) and other security-critical information which may be needed by the system (e.g., such as the user's authorized role).

Detailed Description Text - DETX (8):

The integrity-locked digitized canonical biometric data is hereinafter referred to as "certificate-based alias detection data (CBAD)." The registrar integrity locks the certificate by appending a digital signature to it. A digital signature in its simplest form is simply an **encrypted** copy of the certificate that is **encrypted** using the registrar's assigned private **key** (which is known only to the registrar 110 and the registrar's work station). The digital signature is used with the data to be "integrity-locked" by using the signature to provide an encryptographic checksum or other appropriate code. Appending the digital signature provides "integrity-locked" or digitally signed account/authentication/certificate-based alias detection data 120 where it is stored in the name service program 19. The above mentioned public **key cryptographic** type techniques are used to ensure that tampering of account/authentication/certificate-based alias detection data is detectable.

Detailed Description Text - DETX (9):

At a later time, any entity may verify that the account certificate 130 was, indeed, signed by the registrar 110 by decrypting the digital signature using the registrar's 110 public **key** (which is known throughout the system) and comparing the results with an associated plaintext certificate of the decrypted digital signature. The plaintext certificate is a decrypted version of the digital signature. If they are identical, the entity using the account certificate is confident that neither the plaintext nor **encrypted** versions of the account certificate were modified after they were created or modified by the registrar 110, and that the account certificate data did originate from the registrar's workstation.

Detailed Description Text - DETX (10):

When an individual user logs on to a workstation, the individual user provides information (such as the user's name) that is used by the local operating system to locate and fetch an account certificate from the name service program 19 as the first step in authenticating, or confirming the identity, of the individual user. The local operating system then validates the account certificate's digital signature using the registrar's public **key**. If the account certificate is valid, the public **key** assigned to that account by the registrar 110 is known.

Detailed Description Text - DETX (11):

The individual user trying to log in then presents a digitally signed "login delegation certificate" to the workstation. A login delegation certificate is

what the user sends to the local operating system to be authenticated. (Typically, this would be done by a smartcard issued to the individual user by the registrar 110, containing the individual user's personal private **key.**) The operating system validates the login delegation certificate by decrypting it using the public **key** it obtained from the account certificate. If the validation is successful, the operating system knows that the public **key** obtained from the account certificate matches the private **key** in the possession of the individual user trying to log on, and is justified in assigning to that individual user any rights or privileges associated with the account. At no time during the authentication process is the CBAD data in the account certificate used. Since CBAD data does not determine the success or failure of a login authentication, there is no compromise to the integrity of the login authentication system if CBAD data is public.

Detailed Description Text - DETX (12):

In order to invoke a remote application (e.g., from the application server system 16) to be executed on behalf of, or at the request of, a properly authenticated local user, the workstation operating system generates a so-called remote delegation certificate for the request by appending to the request the individual user's login delegation certificate and digitally signing it using the workstation's private **key**. A remote delegation certificate is what the local computer operating system sends to the applications server system 15 to obtain services on behalf of the individual user. The application server system 16 can then verify that the remote delegation certificate came from the workstation (by applying the workstations public **key** to the signature), and, if this is successful, can reauthenticate the identity of the individual user by verifying the user's signature on the included remote delegation certificate using the user's assigned public **key**. Provided that both of these tests are successful, the application server system 16 knows that the included request emanated from the workstation claimed, acting on behalf of the user account claimed, and/or can use this information to determine whether or not the request should be honored. Since CBAD-data is not used to determine the validity of a remote delegation certificate, there is no compromise to the remote request authentication system if CBAD data is public.

Detailed Description Text - DETX (13):

Each user also has an associated account certificate 130. A user certificate 130 is a data structure, generated by the operating system, that includes user information 120 and CBAD data, if it exists , which are bound together. The binding of these data can be provided by using a **cryptographic** checksum. The checksum ensures that any corruption of the user information 120

is detectable by the system. The **encryption** uses the registrar's 110 private **key or encryption** code, thus generating a digital signature that uniquely identifies the source of the account information as the registrar 110. The account certificate 130 is then posted by the operating system to the name service system 135. Thus, execution of selected tasks can be restricted to selected users or groups of users.